PTO/SB/08a (06-03)
Approved for use through 07/31/2003. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/734,231
Filing Date	Dec 15, 2003
First Named Inventor	PROOS, John A. et al.
Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0466-US

OIPE
FEB 25 2004
PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number	Document Number: Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JV		US- 6,081,597		06-27-2000	HOFFSTEIN, Jeffrey et al.	
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Office[3]	Foreign Patent Document: Number[4]	Foreign Patent Document: Kind[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	9 MAR 07

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08B (06-03)
Approved for use through 06/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	NOT YET SPECIFIED
Filing Date	Dec 15, 2003
First Named Inventor	PROOS, John A. et al.
Group Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0466-US

OIPE
FEB 25 2004
PATENT & TRADEMARK OFFICE

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
[illegible]		PROOS, JOHN A., "Imperfect Decryption and an Attack on the NTRU Encryption Scheme,"University of Waterloo, Waterloo, Canada, January 7, 2003.	

Examiner Signature	[illegible]	Date Considered	9 MAR 07

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE JC25 APR 22 2004 PATENT & TRADEMARK OFFICE

PTO/SB/08B (06-03)
Approved for use through 06/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/734,231
Filing Date	December 15, 2003
First Named Inventor	PROOS
Group Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0466-US

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Consortium for Efficient Embedded Security, EESS #1: Implementation Aspects of NTRUEncrypt and NTRUSign, Version 1, November 2002.	
		HESS, E; JANSSEN, N; MEYER, B; SCHUETZE, T. "Information Leakage Attacks Against Smart Card Implementations of Cryptographic Algorithms and Countermeasures - A Survey", Proceedings of Eurosmart Security Conference, pp. 55-64, Marseilles, 2000, European Smart Card Industry Assoc., 2000.	
		SHAMIR, A. "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies", in Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2000, pp. 71-77, LNCS Vol. 1965, C.K. Koc et al, Eds., Springer-Verlag, 2000.	
		KOCHER, P.C. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", in Advances in Cryptology - CRYPTO'96, LNCS Vol. 1109, N. Koblitz, Ed., pp. 104-113, Springer-Verlag, 1996.	

Examiner Signature		Date Considered	9/14/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.